REMARKS

The Examiner is thanked for the performance of a thorough search.

STATUS OF CLAIMS

Claims 3, 5-8, 12-15, 17, 21-23, 26-27, and 34 have been cancelled.

Claims 1-2, 4, 9-11, 16, 18-20, 24-25, 28-33 have been amended.

Claims 35-54 have been added.

No claims have been withdrawn.

Claims 1-2, 4, 9-11, 16, 18-20, 24-25, 28-33, and 35-54 are currently pending in the application.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 1, 2, 13, 18-26, and 32-34 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent Number 6,687,245 issued to Fangman et al. (" *Fangman* "). Claims 3-9 and 27 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fangman* in view of U.S. Patent Number 6,707,915 issued to Jobst et al. (" *Jobst* "). Claims 10, 12, and 28-29 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fangman* in view of U.S. Patent Application Publication Number 2003/0031151 of Sharma et al. (" *Sharma* "). Claims 11 and 14-17 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fangman* in view of U.S. Patent Number 6,886,103 issued to Brustoloni et al. (" *Brustoloni* "). Claims 30-31 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Fangman* in view *Jobst* and in further view of *Sharma*. The rejections are respectfully traversed.

As a preliminary matter, Claim 13 is listed as part of the group of claims listed in item 3 on page 2 of the Office Action (e.g., the introduction to the rejections under 102(e) based on *Fangman*), yet Claim 13 is not addressed in the detailed action following thereafter or anywhere else that the Applicant could see in the Office Action. Therefore, the Applicant has proceeded on the basis that Claim 13 was intended to be included in the claims listed under item 4 on page 2 of the Office Action. Note that the features of Claim 13 as filed are now included in Claim 10 above with Claim 13 being cancelled.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

"A method for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first node, wherein:

the first node is associated with a first network address;

the first electronic message is based on IPsec;

the first electronic message is associated with a first identifier;

the first identifier is generated by the first node; and

the first electronic message is addressed to a second network address;

the device generating a value based on the first identifier and a specified scheme;

sending the first electronic message to a second node based on the second network address, wherein the first electronic message includes a particular network address that is associated with the device instead of the first network address;

receiving a second electronic message from the second node, wherein:

the second electronic message is based on IPsec;

the second electronic message is addressed to the particular network address;

the second electronic message is associated with a second identifier that is different than the first identifier; and

the second identifier is generated, based on the first identifier and the specified scheme, by the second node;

the device determining whether the second electronic message is directed to the first node based on the value and the second identifier; and

sending the second electronic message to the first node at the first network address when the second electronic message is determined to be directed to the first node." (Emphasis added.)

Thus, Claim 1 features the handling of electronic messages by "a device that employs address translation" in which the device not only performs the normal address translation functions, but also performs additional steps based on the identifiers of the different messages. It appears to the Applicant that the Office Action is confusing the normal network address translation (NAT) functions disclosed in *Fangman* with the Applicant's novel approach for identifying the proper IPsec originator node to which a response message is directed through the use of an identifier, a value determined based on that identifier, a second identifier that is based on the first identifier, and determining that the message is directed to the proper node based on the second identifier and the value. Thus, the Applicant has amended Claim 1 above, along with similar changes to the other independent claims in the application, to positively recite the features of NAT (e.g., the different network addresses and the changes among network addresses), to try to prevent any confusion between such normal NAT functions and the novel use of identifiers and the value. The changes to Claim 1 and the other independent claims are fully supported by the specification as filed, and no new matter is introduced.

For example, in the embodiment illustrated in FIG. 2A and FIG. 2B and described in the application in paragraphs [0039] to [0058], a NAT device handles messages between an IPsec originator node and an IPsec responder node. When the IPsec originator node sends a message to the NAT device, the IPsec originator node includes a randomly generated IPsec safety parameter index (SPI) as the identifier. The NAT device does the normal address translation by replacing the local IP address of the IPsec originator node with the global IP address for the NAT device.

In addition to the normal address translation, the NAT device also performs a hash of the SPI generated by the IPsec originator node, and then stores that hash in the translation table. For example, FIG. 5A, which is described in paragraphs [0098] through [0100] of the application, presents an example of a translation table in which the inside local address 530 for IPsec originator node 410 is appended with the hash of the IPsec originator node's SPI (e.g., the "0xD4560CA1" that is added to the IP address of 10.6.1.2). After the NAT device has performed both the normal address translation function (e.g., replacing the network address of the originator node with the global IP address of the device) plus the additional

hashing of the originator node's SPI, the NAT device sends the message to the IPsec responder node.

When the IPsec responder node receives the message, the responder node does a hash on the originator's SPI that is included with the message. The responder node then generates its own SPI based on a conventionally generated SPI (e.g., randomly generated), plus the hash value of the originator's SPI. As a specific example, the responder node can replace the last two bytes of the responder nodes conventionally generated SPI with the first two bytes of the hash of the originator's SPI as determined by the responder node. See Application, paragraphs [0064] through [0067]. Then the responder node appends the resulting SPI to the global IP address of the originator node/NAT device and sends the message.

Once the NAT device receives the message from the IPsec responder node, the NAT device uses the hash values of the SPIs of any originator nodes that are stored in the hash table and then compares the first two bytes of those stored hash values with the last two bytes of the responder node's SPI. When a match is found, the NAT device knows which originator node the message is supposed to go to, and then the NAT device can perform address translation based on the local IP address for the matching originator node from the translation table so that the message is sent to the correct originator node. Also, the NAT device can make another entry in the translation table that associates the responder node's SPI with the internal IP address of the correct originator node, as illustrated by row 506 in FIG. 5B. Thereafter, any messages from the responder node for that particular matching originator node can be immediately identified as going to that matching originator node based on that newer entry to the translation table.

Note that in the approach of Claim 1, as typified by the embodiment described above, the NAT device is performing both the normal address translation function of changing the local IP addresses of the originator nodes to the global IP address, with corresponding additions to the NAT translation table, along with doing the hash of the originator nodes' SPIs, which are also stored in the NAT translation table. As a result, when a response is received at the NAT device from the responder node, the NAT device can match up the responder node's SPI to the hashes of the possible matching originator nodes' SPIs to determine the right originator node to send the message to. Thereafter, the NAT device makes another entry in the NAT translation table that associates the responder node's different SPIs

for the IPsec communications with each IPsec originator node to preclude the need to perform the matching steps again.

As discussed in the background portion of the application, the novel approach of Claim 1 avoids the problem that arises when two IPsec originator nodes try to establish IPsec communications at about the same time with the same IPsec responder node. When the IPsec communications are being established, the NAT device has not yet made an association with each responder SPI and the corresponding originator nodes' internal IP addresses, and as a result, the NAT device cannot know for sure which IPsec originator node a particular IPsec responder node's response message is to go to. But because the NAT device does the hash on the originator nodes' SPIs as the outgoing messages are sent, and stores those hash values in the translation table, the NAT device can match up the different response messages from the responder node to the different originator nodes. This is possible and secure because the responder node is doing the same hash of the same originator SPI for each IPsec communication setup, and the NAT device knows how the responder node is incorporating part of the hash value of the originator nodes' SPIs into the corresponding SPIs from the responder node.

Note that while the above discussion describes an embodiment of the approach of Claim 1 in light of the particular embodiments described in the application, the approach of Claim 1 is not limited to those embodiments described above or elsewhere disclosed in the application.

(2) INTRODUCTORY DISCUSSION OF *FANGMAN*

In contrast to the approach of Claim 1, *Fangman* discloses an approach for establishing IP telephony based communications, specifically voice over IP (VOIP) calls between phones over the Internet through the use of a service gateway (SG) and a media gateway controller (MGC) and assigning ranges of ports to the IP telephone (IPT). (Abstract.) In particular, *Fangman* is directed to the incorporation of network address translation persistent port translation (NAPPT) in such a system.

While *Fangman* includes discussions of incorporating IPsec based traffic as part of the VOIP approach disclosed herein such as IPsec based virtual private network (VPN) tunnels (see, for example, Col. 8, lines 14-25, Col. 9, lines 24-41, Col. 13, lines 40-46, Col. 24,

lines 6-12, Col. 27, lines 55-60, et seq.), as best understood by the Applicant, *Fangman* does not perform the type of IPsec processing as in the approach of Claim 1 involving identifiers for IPsec nodes and computation of a value, such as a hash value, based on one identifier and the incorporation of part of that value in another identifier, as in the approach of Claim 1, and as discussed in detail below in the remarks concerning the details of the Office Action's rejections.

Rather, *Fangman* is entirely silent as to how the ambiguity that arises from two IPsec nodes behind a NAT device that are trying to establish IPsec communications with the same responder node would be resolved. Thus, as best understood by the Applicant, the approach of *Fangman* merely employs the conventional approaches for handling IPsec communications as discussed in the Background section of the Applicant's specification, and thus *Fangman* remains vulnerable to the problems discussed in the Applicant's background of not knowing which IPsec originator node is to get a particular response message from an IPsec responder node in the particular situations discussed herein.

(3) THE OFFICE ACTION'S CITATIONS FROM *FANGMAN*

In the detailed rejection of Claim 1, the Office Action states that *Fangman* discloses "receiving a first electronic message from a first node, wherein the first electronic message is based on IPsec and is associated with a first identifier; (col 3 lines 65 through line 2 and col 6 lines 30-34 and column 9 lines 24-34 and col 24 lines 60-26 col 18 lines 1-39)(i.e., the examiner interpreted 120A as the first node)" and "generating a value based on the first identifier;(col 4 lines 1-12)."

The Office Action does not specify what in these portions of *Fangman* is being taken as the "identifier" in Claim 1. However, all of these sections of *Fangman* discuss network address translation (NAT) in terms of the private source IP address of the IP telephone, the source port number, the public source IP address of the IP telephone, a public destination IP address, and a destination port number, in which the port addresses are unchanged whereas the IP addresses are changed between public and private addresses in a conventional NAT fashion. Thus, it appears to the Applicant that the Office Action's citations to these sections of *Fangman* is based on one of these addresses or ports corresponding to the identifier of Claim 1.

In particular, the citation to Col. 4, lines 1-12 for the step of "generating a value based on the first identifier" seems to indicate that the Office Action is based on the private source IP address of the IP telephone being the "identifier" of Claim 1 and the "public source IP address" being the "value" that is generated.

The Applicant notes that these IP addresses, whether public or private, are not being generated by the IP telephones or NAT device, but rather these IP addresses are being selected or changed between each other by the NAT device. Typically, the private internal IP address of the IP telephone is already generated and assigned, and similarly the public IP address that the NAT device substitutes for the private address are already generated and assigned when the devices are initially configured. Then it is the normal NAT function to switch the source and destination addresses between public and private IP addresses as part of the normal NAT process.

Thus, the cited portions of *Fangman* do not show the generation of a value based on an identifier (e.g., the generation of the public IP address based on the private IP address), but rather the substitution of the private IP address with the public IP address, both of which are already generated. Therefore, the Applicant respectfully submits that *Fangman's* description of substituting IP addresses fails to show "generating a value based on the first identifier," as in Claim 1.

However, there is an even more fundamental different between these passages of *Fangman* and the approach of Claim 1, as amended above: now Claim 1 features both the typical network address translation features plus the extra features of using two identifiers, a value, and a specified scheme to route messages through the NAT enabled device to properly direct messages to nodes within the network of the NAT enabled device. Specifically, Claim 1 features including the particular network address that is associated with the device instead of the first network address that is associated with the first node, which is akin to replacing the private IP address of the IP telephone with the public IP address of the IP telephone in *Fangman*. In addition, Claim 1 features the first identifier, which is now recited as being generated by the first node, and the value that is generated by the device based on the first identifier and the specified scheme. Thus, while the Applicant believes that the descriptions of NAT in the cited portions of *Fangman* may be considered to correspond to the

normal NAT functions that are now recited in Claim 1, the Applicant fails to see any other features of Claim 1 in *Fangman* that would correspond to the first identifier and value.

The Office Action also states that *Fangman* discloses "receiving a second electronic message from the second node, wherein the second electronic message is based on IPsec and is associated with a second identifier that is different than the first identifier, wherein the second identifier is generated based on the first identifier; (column 9 lines 24-34 and col 24 lines 6-26 and col 18 lines 1-39)." However, as noted above, these portions of *Fangman* are describing typical NAT functions in which private IP addresses are substituted for public IP addresses, which would now correspond to the network address features of Claim 1 as amended above and the changes in same.

The Applicant fails to see anything in these cited portions of *Fangman* that would then correspond to the second identifier being generated by the second node based on the first identifier and the specified scheme, keeping in mind also that the first identifier is recited previously in Claim 1 as being generated by the first node. As noted above, the IP addresses that the NAT device are changing back and forth along with the port numbers are not generated by either the NAT device, nor the IP telephones because such IP addresses are generated elsewhere and assigned to those devices, with the NAT device just making substitutions between IP addresses and assigning port numbers. These descriptions in *Fangman* are unlike Claim 1 in which both the first and second identifiers are generated by the first and second nodes, respectively, along with the generation of the value by the NAT enabled device. Also, note that the first and second identifiers and the value are distinguished expressly in Claim 1 in the above amendments from the network addresses.

The Applicant respectfully requests that any future Office Action clarify what is being relied upon in the prior art as corresponding to the "first identifier" that "is generated by the first node," the "second identifier" that "is generated, based on the first identifier and the specified scheme, by the second node," and the "value" that is generated by "the device" "based on the first identifier and a specified scheme." These features of Claim 1 have three different things (e.g., the first identifier, the second identifier, and the value) being generated by three different entities (e.g., the first node, the second node, and the device). In addition, there are specific interrelationships between these three different things (e.g., that the value is

based on the first identifier, that the second identifier is based on the first identifier, and that both the value and the second identifier are based on the same specified scheme).

As indicated above, the inclusion of the different network addresses for the first and second nodes and the device and the changes above them are intended to distinguish the normal NAT functions, such as those described in *Fangman*, from these identifiers and values. Thus, the Applicant fails to see anything within *Fangman* that correspond to the first and second identifiers and the value, as featured in Claim 1.

Also, the Applicant notes that in Claim 1, the ***same*** "specified scheme" is used by both the NAT enable "device" to generate the value based on the first identifier and the second node in generating the second identifier based on the first identifier. Thus, it appears to the Applicant that if the Office Action is relying on *Fangman's* discussion of the typical NAT functions as showing the generation of the value in Claim 1 (which as explained above does not seem to be proper), then it is unclear to the Applicant how the other devices, such as the IP telephones and specifically the IP telephone that the Office Action expressly states is taken to correspond to the second node of Claim 1, can employ the same NAT function (e.g., the same "specified scheme" in Claim 1). As best understood by the Applicant, the IP telephones in *Fangman* do not perform network address translation like the NAT device does, and thus the IP telephone relied upon by the Office Action as corresponding to the second node cannot use the same "specified scheme" as the NAT enabled device.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *FANGMAN*

Because *Fangman* fails to disclose, teach, suggest, or in any way render obvious "receiving a first electronic message from a first node, wherein: the first node is associated with a first network address; ... the first electronic message is associated with a first identifier; the first identifier is generated by the first node; and the first electronic message is addressed to a second network address," "the device generating a value based on the first identifier and a specified scheme;" or "receiving a second electronic message from the second node, wherein: ... the second electronic message is addressed to the particular network address; the second electronic message is associated with a second identifier that is different than the first identifier; and the second identifier is generated, based on the first identifier and the specified

scheme, by the second node," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

(5) DISCUSSION OF CLAIM 1 AND *JOBST*, *SHARMA*, AND *BRUSTOLONI*

Although the rejection of Claim 1 relies only upon *Fangman*, the Applicant wishes to address the other cited prior art references used in the rejections of other claims to explain why the Applicant believes that none of those prior art references, either alone or in combination with each other or *Fangman*, disclose the approach of Claim 1 as amended herein. The Applicant notes that the Office Action relies upon these prior art references for additional features of other claims that generally are not included in Claim 1, but the Applicant nevertheless will briefly address why none of these other prior cited art references disclose the features of Claim 1, as amended above.

The Applicant notes that these references may indeed show elements that are apparently the same as in corresponding dependent claims (e.g., hash functions, MD5, and the various features of IPsec such as SA's, SPI's, and ESP's), although the Applicant does not agree that the mere mention of these features in such prior art references discloses the features as being combined and used in the same way as in the claims as recited therein or that it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to combine such features, little less how such features could be combined in the manner featured in the claims of the present application.

Jobst is relied upon by the Office Action as disclosing the features of Claims 3-9, 27, 30, and 31, citing "col 7 line 23 through line 27 and col 10 line 50 through col 11 line 15" and "col 8 lines 50-59." In particular, the Applicant notes that features similar to those of Claim 3, now cancelled, have been incorporated into Claim 1 above.

The first cited portion of *Jobst* addresses the calculation of a phone password based on a secure hash algorithm, such as MD5, and in particular, that section describes that phone password 40 is outputted from the hashing based on using the IME code 37 and the Master Password 38 as inputs. The second cited portion of *Jobst* describes verifying signatures, and in particular, a first signature 43 is determined by phone 1 using a secure hash algorithm 42, such as MD5, based on a phone password 45 and a binary code 47, while second signature 46 is determined by phone 1 using the same secure hash algorithm 42 and a code image 47 and

the phone password 45, and that software provider 33 calculates the first signature 43 based on the code image 44, the IMEI code 37, and master password 38.

Again, it is unclear to the Applicant exactly which of these elements of *Jobst* are being relied upon as corresponding to the features of Claim 1, and in particular, what corresponds to the "first identifier," "second identifier," and the "value" of Claim 1. For example, one possibility is that the two signatures 43 and 46 calculated by phone 1 correspond to the two identifiers of Claim 1 and the signature 43 calculated by the software provider corresponds to the value of Claim 1. The problem is that results in an inconsistency with Claim 1 that specifies that the first identifier is generated by the first node and the second identifier is generated by the second node based on the first identifier, where as *Jobst* has phone 1 calculating both signatures 43 and 46 and neither is determined based on the other.

Another possible matching of these elements of *Jobst* to the features of Claim 1 is that master password 38 is being relied upon as the "first identifier" and that first signature 46 as calculated by the software provider 33 is the "second identifier" since the master password 38 is used by software provider 33 in generating first signature 46. But *Jobst* in the portion from column 7 says that master password is determined by certification center 35, not an IP telephone, and thus would be inconsistent with the Office Action relying on the first and second nodes corresponding to IP telephones.

Furthermore, the Applicant is unable to find in either these cited portions of *Jobst* or elsewhere within *Jobst* any elements that would correspond to the "first identifier" that is generated by the first node, the "second identifier" that is generated by the second node based on the specified scheme and the first identifier, and the "value" that is determined by the NAT enabled "device" based on the first identifier and the specified scheme. The Applicant notes that the first identifier and the specified scheme are used by both the device and the second node in Claim 1, but the device determines a value while the second node determines an "identifier," with both subsequently being used by the device to determine that a message from the second node is to go to the first node. Yet the Applicant fails to see any corresponding disclosures of these features of Claim 1 in *Jobst*. Therefore, the Applicant respectfully submits that Claim 1 is allowable over *Jobst*.

Sharma is relied upon by the Office Action as disclosing the features of Claims 10, 12, and 28-31, citing paragraphs [0025], [0030], and [0062-0063]. Paragraph [0025] describes

IPsec security associations (SAs) and the use of encapsulating security payloads (ESPs) for secure virtual private networks (VPNs) as involving new IP headers that contain routable addresses of security gateways because tunneling may high original source and destination addresses. Yet such a disclosure says nothing about the "first identifier," the "second identifier," and the "value" as featured in Claim 1.

Paragraph [0030] describes the creation of IPsec SAs through the use of the Internet Key Exchange (IKE) protocol that includes the use of security parameter indexes (SPIs) for identifying the previously agreed upon algorithms and keys of the particular SAs between IPsec nodes. Yet again, this disclosure from *Sharma* says nothing about the "first identifier," the "second identifier," and the "value" as featured in Claim 1.

Paragraphs [0062-0063] describe a key exchange to establish a secret key and a SPI to identify that key, along with the use of a MD5 hash function of the key as an authentication value. But yet again, this disclosure from *Sharma* says nothing about the "first identifier," the "second identifier," and the "value" as featured in Claim 1. Therefore, the Applicant respectfully submits that Claim 1 is allowable over *Sharma*.

Finally, *Brustoloni* is relied upon by the Office Action as disclosing the features of Claims 11 and 14-17, citing "col 6 lines 40-45," "col 6 line 57 through col 7 line 14 and col 7 line [?] col 8 line 7," and "col 7 lines 34-50." The discussion from bottom portion of Column 6 through Column 7 to the top of Column 8 in *Brustoloni* describes the accommodation of IPsec that is not supported by a NAT enabled device via the "Unsupported-Protocol Module 110." However, the Applicant notes that *Brustoloni* says that "IPSec AH and ESP protocols in both the transport and tunnel modes" "is not or cannot be directly supported by the NAT." (Col. 6, lines 57-63.) Thus, *Brustoloni* says that a "client-implemented ALG" (Application Level Gateway)" is needed "to perform necessary modifications in packet payloads to compensate for NAT translations." (Col. 6, lines 64-66.) Thus, *Brustoloni's* approach is fundamentally different than that of Claim 1 because *Brustoloni* says that a NAT enabled device cannot support these features of IPsec, whereas the approach of Claim 1 is to enhance a NAT enabled device to support such features of IPsec. Furthermore, the Applicant points out that Claim 1 includes features that recite functions performed by the first node (e.g., generation of the first identifier), the second node (e.g., generation of the second identifier based on the first identifier), and generating a value by the

device that employs NAT. But in *Brustoloni*, the approach is to use a "client-implemented" ALG, meaning that the functions of that ALG are only at the client and not at the NAT device, which is different than in the approach of Claim 1.

Furthermore, the cited portions of *Brustoloni* describe the uses and changes among IP addresses, whereas in Claim 1, the network addresses and normal NAT functions are expressly distinguished from the generation and use of the two identifiers and the value. Thus, as with *Jobst* and *Sharma*, *Brustoloni* says nothing about the "first identifier," the "second identifier," and the "value" as featured in Claim 1. Therefore, the Applicant respectfully submits that Claim 1 is allowable over *Brustoloni*.

As noted above, the Applicant respectfully requests that any future Office Action explain which features of *Jobst*, *Sharma*, and/or *Brustoloni* are being relied upon as showing the features of Claim 1, particularly the elements being relied upon in the prior art references, whether those that have been cited or others that may be cited, as disclosing the "first identifier," "second identifier," and the "value."

C. CLAIMS 24-25, 30, 32, 33, 35, AND 45

Claims 24-25, 30, 32, 33, 35, and 45 contain features that are either the same as or similar to those described above with respect to Claim 1. For example, Claims 32, 35, and 45 all feature "receiving a first electronic message from a first node, wherein: the first node is associated with a first network address; ... the first electronic message is associated with a first identifier; the first identifier is generated by the first node; and the first electronic message is addressed to a second network address," "the device generating a value based on the first identifier and a specified scheme;" and "receiving a second electronic message from the second node, wherein: ... the second electronic message is addressed to the particular network address; the second electronic message is associated with a second identifier that is different than the first identifier; and the second identifier is generated, based on the first identifier and the specified scheme, by the second node," which is the same as in Claim 1.

As another example, Claims 24 and 33 both feature "receiving a first electronic message from a first node, wherein: the first node is associated with a first network address; ... the first electronic message is associated with a first identifier; the first identifier is generated by the first node based on a second identifier and a specified scheme; ... and the

first electronic message is addressed to a second network address," "the device generating a value based on the second identifier and a specified scheme;" and "receiving a second electronic message from the second node, wherein: ... the second electronic message is addressed to the particular network address; the second electronic message is associated with the second identifier; and the second identifier is generated by the second node," which is similar to Claim 1.

As yet another example, Claim 25 features "receiving, from the device that employs address translation, a first electronic message that originates from the first node, wherein: ... the first electronic message is associated with a first identifier; the first electronic message includes a particular network address that is associated with the apparatus instead of a first network address that is associated with the first node; and the first electronic message is addressed to a second network address that is associated with the second node," "the apparatus generating a second identifier based on the value and the specified scheme;" and "generating a second electronic message to the first node, wherein: ... the second electronic message is associated with the second identifier; and the second electronic message is addressed to the particular network address," which is similar to Claim 1.

And as a final example, Claim 30 features "receiving a first electronic message from a first IPsec originator node, wherein: the first IPsec originator node is associated with a first network address; ... the first electronic message is associated with a first security parameter index (SPI); the first SPI is generated by the first IPsec originator node; and the first electronic message is addressed to a third network address," "the router generating a first hash value based on the first SPI and a hash algorithm;" "receiving a second electronic message from a second IPsec originator node, wherein: the second IPsec originator node is associated with a second network address; ... the second electronic message is associated with a second SPI; the second SPI is generated by the second IPsec originator node; and the second electronic message is addressed to the third network address," "the router generating a first hash value based on the first SPI and a hash algorithm;" "the router generating a second hash value based on the second SPI and the hash algorithm;" and "receiving a third electronic message from the IPsec responder node, wherein: ... the third electronic message is associated with a third SPI that is different than the first SPI and the second SPI; the third electronic message is addressed

to the particular network address; and the third SPI is generated by the IPsec responder node based at least in part on the hash algorithm;" which is similar to Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 24-25, 30, 32, 33, 35, and 45 are allowable over the art of record and are in condition for allowance.

D. CLAIMS 2, 4, 9-11, 16, 18-20, 28-29, 36-44, AND 46-54

Claims 2, 4, 9-11, 16, and 18-20 are dependent upon Claim 1, Claims 28-29 are dependent upon Claim 25, Claims 36-44 are dependent upon Claim 35, and Claims 46-54 are dependent upon Claim 45. Each of Claims 2, 4, 9-11, 16, 18-20, 28-29, 36-44, and 46-54 is therefore allowable for the reasons given above for Claims 1, 25, 35, and 45. In addition, each of Claims 2, 4, 9-11, 16, 18-20, 28-29, 36-44, and 46-54 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2, 4, 9-11, 16, 18-20, 28-29, 36-44, and 46-54 are allowable for the reasons given above with respect to Claims 1, 25, 35, and 45.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: January 6, 2006

Craig G. Holmes
Reg. No. 44,770

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on Jan. 6, 2006 by Tracy Reynolds